

# Introduction

## Welcome to the Upgrade

Welcome to NFC's applications Upgrade. Combining the proven capabilities of NFC's existing systems with the ease of use of a Windows® environment and the ability to conduct business over a secured telecommunications network, this suite of programs provides you with the tools you'll need to accomplish your personnel, payroll, and administrative processing. Included in the Upgrade are:

- EARN: The Statement of Earnings and Leave System
- EMCP: The Employee System (used with PODS)
- EPIC: The Entry Processing Inquiry and Correction System
- FAAD: The Federal Assistance Awards Data System
- PODS: Personnel Office Desktop Solutions
- PRMS: The Permissions System (used with PODS)
- WTWO: The W-2 System



## Ready . . . Set . . . Upgrade!

To provide its customers with the best possible service, NFC is compelled to change as technology changes. As with any change, making the transition from old to new systems can be challenging, which is why we've created this guide. Each of the applications mentioned here will use the NFC Logon client to connect to NFC and operate. In the sections to follow, we'll cover everything from preparing your site's connection, to logging on to NFC and starting the new applications.



## Basic Steps to Connection

Below you'll find the recommended order for accomplishing your connection to and use of the Upgrade applications. Take a look at the list, then proceed to [Getting Started](#).

- Ensure that site hardware meets minimum system requirements
  - Establish a secured TCP/IP Link to NFC
  - Request access to download client software
  - Obtain NFC Security access for users
  - Download the client software
  - Install the NFC Logon client
  - Install the Upgrade application client(s)
  - Run the NFC Logon client
  - Start the desired Upgrade application.
-



Goto Section:   1   [2](#)   [3](#)   [4](#)   [5](#)   [6](#)   [7](#)   [8](#)   [9](#)   [10](#)   [11](#)   [12](#)   [13](#)

# Getting Started

## Your System Setup

Computer	486 Processor
Operating System	Windows 95/98 or NT 4.0 or higher
Monitor	SuperVGA display (w/ 800x600 resolution or greater)
Telecommunications	Transmission Control Protocol/Internet Protocol (TCP/IP) stack Secure TCP/IP connectivity with NFC
Client Software	NFC Logon software NFC Upgrade Application software
Miscellaneous	Mouse or other pointing device

Hardware and telecommunications should be in place before contacting NFC for an ID and password to download the client software. Questions should be addressed to the customer's agency Information Technology (IT) personnel.

Setting the screen resolution to 800x600 will display the application screens in their entirety. Older monitors and video cards support only VGA (640x480) resolution. If the equipment being used does not support Super VGA (SVGA) resolutions (e.g., 800x600), the agency will need to upgrade to one with that capability. Check with agency IT personnel for more information on monitor compatibility.

The TCP/IP Stack enables applications to communicate with NFC via a TCP/IP network such as the Internet, an intranet, or leased lines. For more information on securing connections to NFC, see [Appendix A](#).

If you've already established a secured TCP/IP link to NFC, you may skip ahead to [Downloading the Client Software](#). If not, please proceed to [Preparing the Connection](#), where we'll cover how to establish secured telecommunications with NFC.



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Preparing the Connection

[Establishing a Secured Link to NFC](#)

[Obtaining Application Security Access](#)

[Summary](#)

---



## Establishing a Secured Link to NFC

To maintain the highest possible protection of customer information, Federal government regulations require that all TCP/IP connections from the agency to NFC be secured. This means that measures must be taken to protect data transmissions from unauthorized access.

To start the process for establishing connectivity between the agency and NFC, a telephone conference must be scheduled between the agency IT specialists, the agency coordinator, and the appropriate NFC officials to discuss the agency implementation strategy and plan. The agency coordinator is responsible for scheduling these telephone conferences, during which both parties should determine which type of connection best suits the needs of the agency.

### Choose the Type of Secured Connection

There are five primary methods for accomplishing this security. Listed below are these methods, as well as a description of the procedures and requirements for each. Additional information may be found in [Appendix A: Connecting to NFC Via TCP/IP](#).

[A. Firewall to Firewall](#). Customer has an Internet Protocol Security (IPSEC) protocol suite-compatible firewall at their site and wishes to connect to NFC's IBM Firewall (Version 4.2) to utilize applications. Currently operating: IBM Version 4.2, Raptor, and Checkpoint Firewall 1 (VPN1).

- **IBM Firewall to IBM Firewall (version 4.2)** – Both firewalls must be at the same level and must be IPSEC compatible. Version 4.2 is Y2K compliant.
- **Checkpoint Firewall to IBM Firewall** – Checkpoint Firewall 1 , Version 3.0 B, Build Number 3072, Virtual Private Network (VPN) plus Data Encryption Standard (DES) or higher version.
- **Raptor Firewall to IBM Firewall** - Raptor Eagle, NT Version 5.0.3.
- **Checkpoint Firewall to Checkpoint Firewall** - Both firewalls must be at Version 4.0.

[B. Gateway to Gateway](#). Customer has a gateway on their network and wishes to connect to NFC's TimeStep/PERMIT Gateway to utilize applications. Currently operating: TimeStep/PERMIT Gateway at customer site.

[C. SecuRemote Client to Checkpoint Firewall](#). Customer may request a SecuRemote Client and access to NFC via TCP/IP through the proper management channels and the NFC Security Officer. The request must include the users NFC ID, e-mail address, and phone number. The client will be given direction on how to download and install the software.

[D. Entrust/SecuRemote Client to NFC](#). For customers who want the added authentication of a Digital Signature to their connection, they may request an Entrust/SecuRemote Client and access to NFC via TCP/IP through the proper management channels and the NFC Security Officer. The client will be given directions on how to download and install the software, and how to activate the digital signature certificate.

[E. Direct Connection \(Line/Router\)](#). Customer has a true private network connection via an onsite Cisco router that connects to NFC's Cisco router to utilize applications. Currently operating: Point-to-Point 56K line, and Point-to-Point T1 line.

## Set Up the Secured Link

Once the method of connection has been coordinated between the agency and NFC, implementation may begin. [Appendix A](#) contains an implementation plan for each method.

---



## Obtaining Application Security Access

Once the telecommunications link is secure, individual user access may be established. This is the traditional "system" security with which most users are familiar. The agency Security Officer should either Email or FAX a request for security access to NFC. Access should be requested based on the application(s) used. For information on what to request, see the [application-specific](#) section of this guide and reference the application(s) for which access is required.

SPECIAL CASE: Customer agencies participating in Quality Assurance (QA) testing for new applications require access to both the QA and production environments. For this to work successfully, the customer must have two IDs - one for production access and one for QA access. For example, each user will need NFXXX (for production only) and NFXXXT (for QA only).

Questions concerning the required security profiles for each user ID may be referred to NFC's Information Systems Security Office at (504) 255-5407.

---



## Summary

When your connection is secured and your application access is established, you're ready to begin [Downloading the Client Software](#).

---

Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Downloading the Client Software

NFC software is available from the File Transfer Protocol (FTP) site, which can be accessed directly from the NFC home page or through the use of a separate FTP client. This site is known as the Download Center. Application setup files may be downloaded to a local PC and installed from there. The programs use an installation procedure similar to that of most other Windows 9x or Windows NT 4.0 applications.

[Getting Access to the Software](#)

[Downloading Files](#)

[Valid Application Downloads](#)

[Summary](#)

---



## Getting Access to the Software

To download software from NFC, the agency Security Officer or IT coordinator obtains an ID and password to the Download Center. This ID accesses the appropriate remote directory from which the desired application setup files may be downloaded. The form used to request the ID is an **AD-1128, Request for Electronic Downloading of Software From NFC**.

For a copy of this form, contact DAB or complete an [online version](#) from the Download Center page. You will need Adobe Acrobat Reader to view and complete the online form. Once completed, it may be mailed, faxed or e-mailed to:

---

Directives and Analysis Branch (DAB)  
National Finance Center  
P.O.Box 60000  
New Orleans, LA 70160

Email: [nfc.dab@usda.gov](mailto:nfc.dab@usda.gov)  
Fax: 504-255-4367

---

Once NFC has processed the request, the agency will receive [software download instructions](#) for accessing the download center. Included are the host name of the download center, the authorized ID and password used to access the specified system folder, and instructions on obtaining and running the application setup files.

---

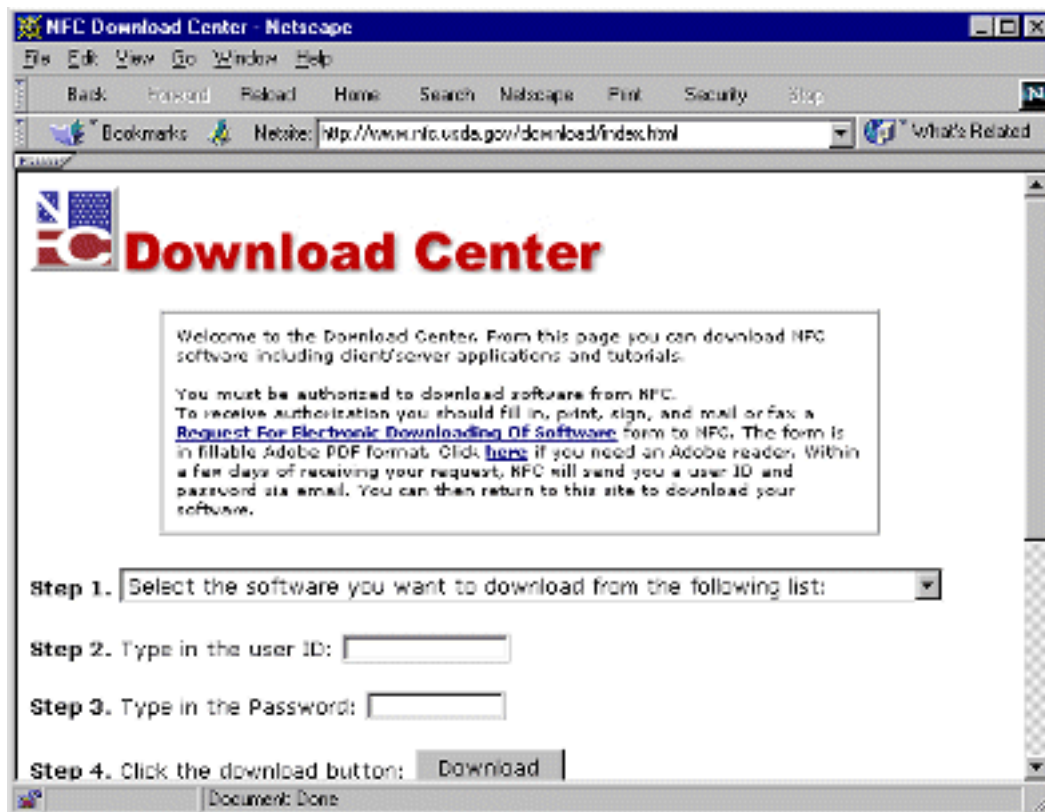


## Downloading Files

There are two ways to download the installation files. The first uses NFC's existing web home page to locate and access the FTP server. The second uses a separate FTP Client to access the server. Both methods require the authorized ID and password discussed above.

### Using the NFC Home Page

To reach the download site, go to the NFC Home page and click the [NFC Download Center](#) button to display the following page:



From this page, you may:

- View, fill-out and print the Form AD-1128 requesting the download ID and password.
- Obtain a copy of Adobe Acrobat Reader to view the form.

And, if you've already requested and received your ID and password

- Select and download the desired software and/or installation instructions.

In Step 1, click the down arrow to view the available applications, shown here:

Select the software you want to download from the following list:

Payroll/Personnel Systems:

NFC Logon System v01.01  
 (EARN) Earnings and Leave Statement System v01.01  
 (EARN) Earnings and Leave Statement System v01.01 Tutorial  
 (EMCP) Employee System v01.01  
 (EPIC) Entry, Processing, Inquiry, and Correction System v01.05  
 (EPIC) Entry, Processing, Inquiry, and Correction System v01.05 Tutorial  
 (PODS) Personnel Office Desktop Solutions System v01.05  
 (PRMS) Permissions System v01.01

Procurement Systems:

(PCMS) Purchase Card Management System v3.1  
 (PCMS) Purchase Card Management System v3.1 Standalone  
 (PCMS) Purchase Card Management System v3.1 Patch

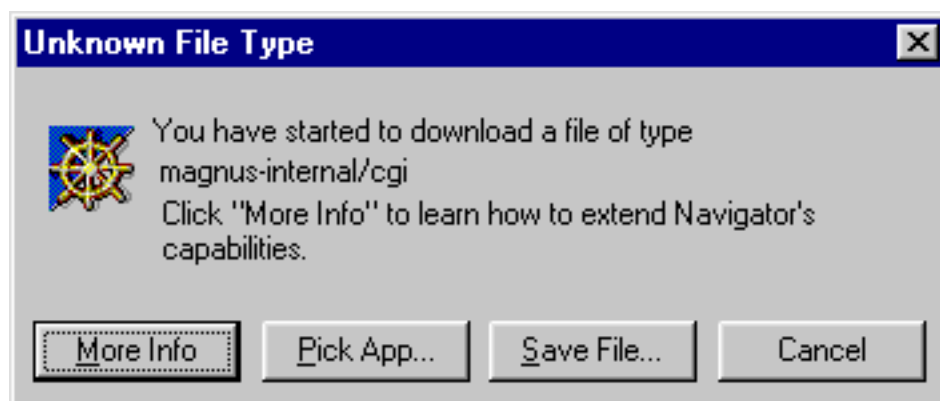
Click to select the desired application.



When you've entered your ID and password, click Download. The following warning message will appear:

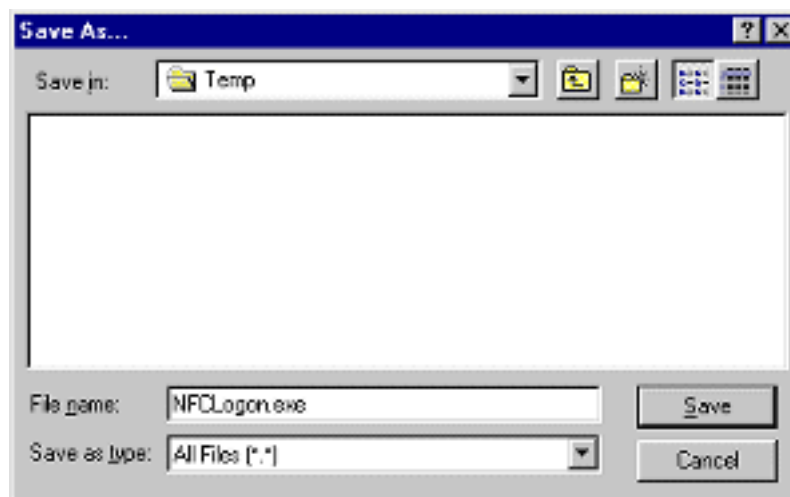


Clicking OK will launch your browser's download file dialog. Depending on your browser configuration you may see a window like this:

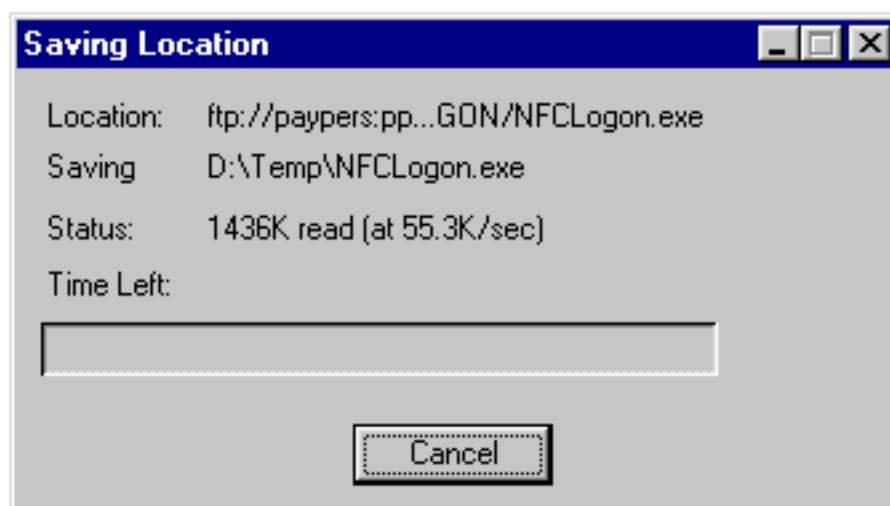


Click Save File... You'll see the Save As... dialog box, and the application filename will appear in the File name: block. Locate the folder to which you wish to save the file, then click Save.





The Saving Location dialog box appears. When the download is complete, this box will close, and you'll be returned to the NFC Download Center page, where you may download another application, or close your browser. Follow the instructions for the selected application to install the software you have downloaded. General installation instructions are discussed in [Installing the Client Software](#).



## Using an FTP Client

If you have an FTP client, you may connect directly to the NFC FTP Server without using a web browser. On the Instruction Sheet you receive from NFC, you will find the following information:

- Host Name
- Authorized User ID
- Case-sensitive password

Use this information to configure your FTP client for connection. Consult your FTP client's help facility for information about using the client.

Some agency Security Officers or IT coordinators may not have FTP client software. If so, WS-FTP Limited Edition, a free-for-government-use FTP client developed by Ipswitch, Inc., may be downloaded from that

[company's website.](#)

---



## Valid Application Downloads

The following are application downloads currently available for each of the listed upgrade systems. They may be accessed from the FTP server as indicated in the section on Downloading Software. Except where noted, all of the applications listed here require the NFC Logon client to run.

Table 1: Applications and Download Filenames

Application	Setup File	Online Tutorial
NFC Logon	NFCLogon.exe	N/A
EARN	Earn0101.exe	EarnTut.exe
EPIC	Epic0105.exe	EpicT105.exe
PODS	Pods0105.exe	PodsTv01.exe
EMCP	Emcp0101.exe	N/A
PRMS	Prms0101.exe	N/A
FAADS	Faw0102.exe	FawT102.exe
WTWO	Uuw0101.exe	UuwT101.exe



## Summary

Once you have all the installation files you require, you may use Windows Explorer to locate the download folder you selected, and follow the steps covered in [Installing the Client Software](#).

---

Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Installing the Client Software

[Installing the NFC Logon Client](#)

[Installing the Application Clients](#)

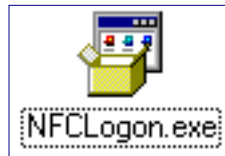
[Summary](#)



## Installing the NFC Logon Client

The NFC Logon allows a customer to access all new NFC application(s), and must be installed first. Although the Logon Client is used to access multiple NFC application(s), it is only installed once per workstation. To install the Logon:

- If Windows 95/NT 4.0 isn't running, start it now.
- Locate the downloaded NFCLogon.exe file using Windows Explorer.



- Double-click the file. This will decompress the software and initiate the setup routine.

OR

- From your taskbar, go to START > Run and enter the drive and filename of the downloaded file, or Browse to find it. Select the file, then click OK to run it.

Follow the on-screen prompts to complete the installation. A typical install runs as shown in Table 1.

Table 1: Installation Sequence	
Screen	Action(s)
Setup	Wait...
Welcome	Click Next.
Select Program Folder	Accept the default program folder (National Finance Center); click Next.
Settings	Review the "Install To" folder and user information and if correct, click Next. To modify any of the information, click Back.
Start Decompressing Files	Wait while setup installs the application components to the selected folder and creates icons. You will be notified when the process is completed.
Setup Complete	You may choose to review the ReadMe file, launch the application, or simply close the Setup window . Make your selection, then click Finish.

The NFC Logon setup file creates an icon in the Start Menu for each PC on which it is run. Once the application clients are installed (see below), and the user has logged in (see [The NFC Logon Client](#)) and checked both the connectivity and security access to the application(s), the original download file (e.g., NFCLogon.exe) may be deleted from the PC or local drive.



## Installing the Application Client(s)

Now that the Logon Client is installed on the customer's PC drive, any of the application clients that have been downloaded may be installed. These include, but are not limited to, EARN, EPIC, PODS, EMCP, and PRMS (for full names of all systems currently available, see the [Introduction](#)). Application clients are installed using the same type of setup utility as the Logon, except that applications may be installed on a Network or on a PC.

### Installing on a Standalone Computer

The setup program for each application is set to install files to a default location of C:\USDANFC\NFCApps. If an agency wishes to load the full application to each individual workstation, they should keep this default location, or change the location to another local hard drive (e.g., a physical drive C, D, etc.). To install the application clients:

- Close all Windows applications
- Use Windows Explorer to locate the application setup program downloaded from NFC's FTP server.
- Double-click the downloaded file.
- Follow the online instructions provided by the setup program, using the Typical setup type.

### Installing to a Network Folder

If an agency wishes to install the application clients to the Network, ensure the person installing the application clients to the network server has write access to that drive and folder. The installation can then proceed as follows:

- Install the application using the instructions under "Installing on a Standalone Computer".
- When the setup program displays the suggested installation drive and directory, change this to the Network server's drive. For example, to install applications to a Network drive called "H", the typical destination location might be: H:\USDANFC\NFCApps
- Continue with the standard installation.
- When the install is completed, click Finish to close the setup window.

### Note on Installing Multiple Application Clients

As a general rule, all application clients should be installed to the same directory. This takes full advantage of the Logon Client's application path selection. When you login to NFC, the Logon client checks the specified path for any installed applications. The default path is C:\USDANFC\NFCApps. For a network install, this would need to be changed to the destination location chosen during the setup. The flexibility comes in when you have users who use only Payroll/Personnel or Administrative systems, or users whose only responsibility is to administer the systems (i.e., users of Permissions, Employee, etc.).

By installing these similar types of applications to their own folders (e.g., NFCApps\Paypers, NFCApps\Admin, NFCApps\Utility), you make it possible for users to see only those applications that pertain to their work.

---



## Summary

With the clients installed, you're ready to start using the applications. As you'll see in the next section, [the Logon client](#) allows you to store up to ten application paths, so even if you have a single PC that is used by several people, you can make it possible for them to customize their Logon session.

---

Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# The NFC Logon Client

The client setup files that were run during installation did several things. First, the program files needed to connect your remote PCs to NFC's telecommunications bridge were loaded. Second, the application runtimes were stored in the specified directories. And, finally, icons were created to allow you to start the Logon client. Because the NFC Logon allows you to access all of NFC's client/server applications, it is the only shortcut you'll need to remember.



[Starting the NFC Logon Client](#)

[Using the Logon Client](#)

[Summary](#)

---



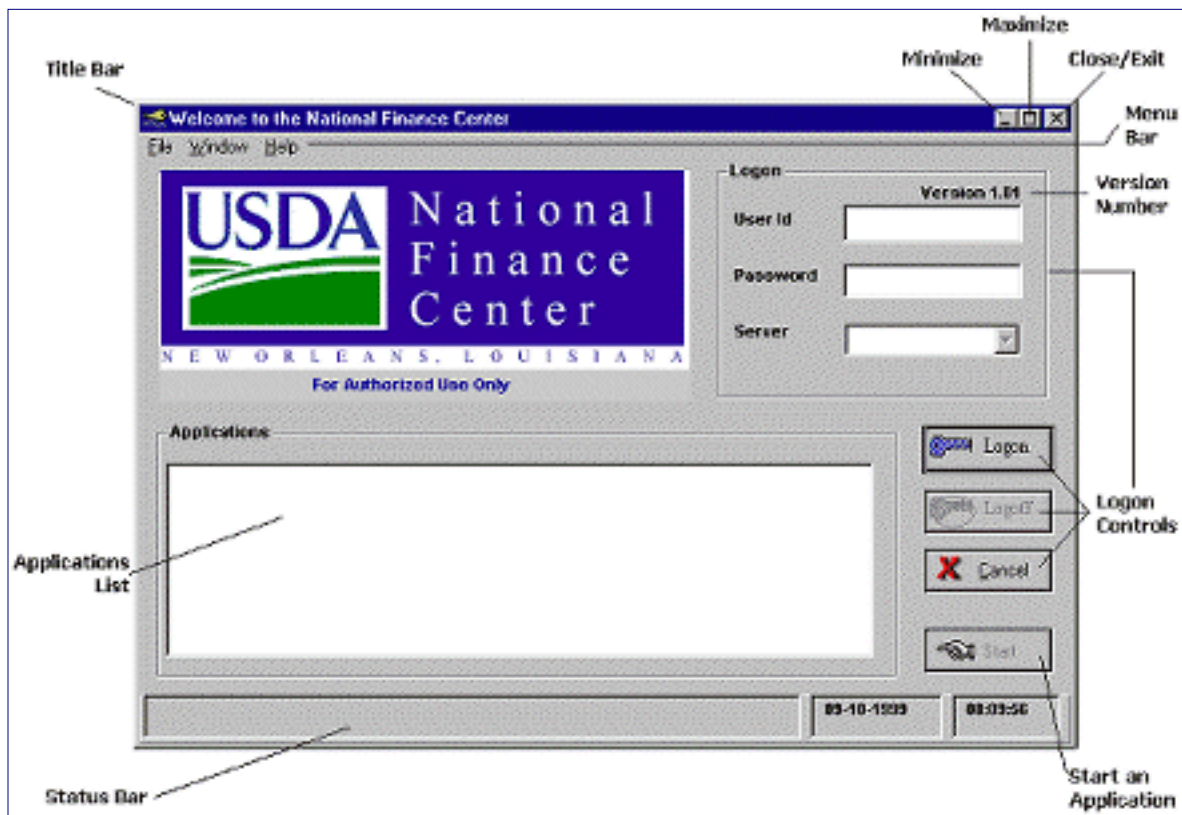
## Starting the NFC Logon Client

If you don't have a shortcut on your desktop like the one above, you may use the Start Menu to open the application:

- Click the Start button on the Taskbar. The Start menu opens.
- Choose Programs. The Programs folder opens.
- Choose National Finance Center. The National Finance Center folder opens.
- Double-click NFC Logon.

## The NFC Logon Window

When you start the NFC Logon, the banner window appears. This window is the launch pad for all NFC Upgrade systems.



## What's on the Banner Window?

### Title Bar

The Title Bar displays the program control icon, the application title, and the minimize, maximize, and close buttons. To access the Control Menu, click once on the control icon in the title bar.



### Menu Bar

The Menu bar displays the menu headings (File, Window, Help). Of note is the Help option, which offers information on the Logon window, general Windows functionality, and a new feature to help determine the version number of each application client. See *Using the NFC Logon Client: Starting an Application* for more information on the "About This Window" function.

### Logon Controls

The Logon controls are grouped into two parts. The first allows the user to enter an NFC ID and password, and to select the server to which they wish to connect. The server options include:

Administrative	Used for regular Production access to systems within the Administrative Payments system
Payroll/Personnel	Used for regular Production access to systems within the Payroll/Personnel system.
Training	Used for accessing the training database.
Parallel 1 and 2	Used during Parallel Testing for new agency implementations.
QA Testing	Used during Quality Assurance testing of new applications.
Test4 and 9	Used by NFC personnel for development.

### Applications List

When Logon is clicked and access to NFC is verified, the applications list displays all available applications in the specified application path. The default path is C:\USDANFC\NFCApps. If the applications were installed in a directory other than the default, you'll need to change the application path to see them in the list (see Application Path). To start one of the applications, click once to select it from the list, and click Start, or double-click the application name.

### Start Button

This button starts a selected application.

### Status Bar

This bar displays system messages like "You have successfully logged into NFC", as well as the local system date and time.



## Using the NFC Logon Client

From this window, users may change their password, modify the Application Path used to access installed application clients, connect to NFC, and start any installed applications. Remember, security access to each application must be obtained for each user, and the logon password must be valid. (See [Troubleshooting](#)).

### Changing Your Password

- To change the Password, click File > Change Password. Type the new password, confirm the change, then click OK. This will modify the system password.

### Application Path

- IT PERSONNEL: If a Destination Location other than the default is chosen during installation, click File > Application Path, and change the path to match the one specified in the install. Following the earlier example, type in an application path of "H:\USDANFC\NFCApps" to access application clients installed to the specified Network drive. You may store up to ten paths in this window. See [Technical Information](#) for more on using this feature.
- END USER: If you receives an application message stating that no applications were found in the application path, contact the agency IT Support to determine the proper path.

### Logging On



- Once the application client path is specified, users can login to NFC. Type the User ID and password, make sure the proper server is selected, then click Logon.
- Each user is logged into the first available NFC server. The logon client then checks the path for installed applications, and displays them in the Application block.

## Checking the Application Version

- On the Logon client window, select an application (e.g., EARN, EPIC, PODS, etc.) from the list box.
- With the application highlighted, click Help > About this Version to activate a readme file containing the client's version information. Check the version number against the Current Version listed on this website to determine if you need to upgrade.

NOTE: If you receive a message to upgrade your application, the NFC Logon has determined that you are running a version of the application that will be replaced within two weeks. Upgrade as directed by the message. See [Troubleshooting](#) for more information.

## Starting an Application

- With the application highlighted, click Start.
- The banner for the selected application appears. At this point the user is logged into the application and may begin working. Consult the application online help and tutorials for more assistance in operating each application.

## Exiting the System

- To exit new NFC applications, close any open system windows and return to the opening application banner. Then click File > Exit from the menu, or the "X" button in the upper right corner of the screen. Either method will close the application. If finished working in NFC applications, terminate the NFC connection by clicking Logoff on the NFC Logon window.



## Summary

With all the clients installed and the Logon Client up and running, you could start using the applications now. But first, we thought you could use some information on [system maintenance](#), including how to update your software or remove an application. Let's take a look.

---

Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# System Maintenance

As systems grow and enhancements are requested, periodic updates may be provided by the NFC. When this happens, it is important to distinguish between the two types of updates: production fixes and new versions.

[Production Fix vs. New Version](#)

[Removing an Application](#)

[File Naming Convention](#)

[Summary](#)

---



## Production Fix vs. New Version

If NFC releases a production fix or patch to an existing version of an application, the new application install should be run to update system files already loaded.

If a new version is released, NFC will notify users that they must obtain and install the new version by a certain date (usually two weeks from the date the version was released). Once installed, the new version is ready to be used on the date it becomes effective. This allows users to install the new version prior to its effective date, and still use the older version until the effective date is reached. At that time, the old version will no longer work, and may be removed so that only the new version is available for use.

### **Installing a Production Fix for an existing application client**

Run the update installation file as described under Installing the Application Client(s). Be sure to use the same setup type and destination location that was used when the original application was installed.

### **Upgrading to a New Version of an existing application client**

Run the update installation file as described under Installing the Application Client(s). When the old version has expired, remove it from the PC as described under "Removing an Application Client." (Note: When removing the client, take note of the Version number in the List Box title...make sure the version removed is the older version.)

---



## Removing an Application

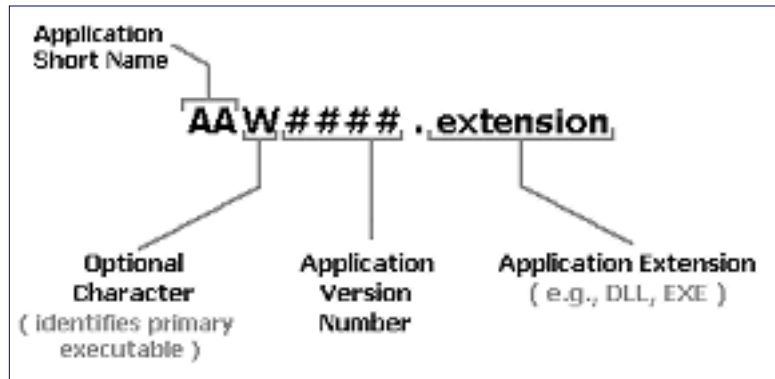
To remove all files that the individual application setup program loaded during installation and to delete the initial Registry entries created during the setup, use the following procedure:

- From the Windows Start menu, choose Settings > Control Panel.
  - In the Control Panel dialog box, double-click Add/Remove Programs.
  - In the list box in the Add/Remove Programs Properties dialog box, select the application to remove (e.g., NFC EPIC v01.01).
  - Click the Add/Remove button.
  - In response to the confirmation message that appears, click Yes (or Yes To All).
-



## Naming Convention for NFC Application Clients

All NFC application files are named based upon a a predetermined standard, as follows:



The application short names and associated file types are:

Application	Short Name	Primary Executable	Sample Program DLL
EARN	EN	ENW0101.exe	EN0101A.dll
EMCP	EC	ECW0101.exe	EC0101A.dll
EPIC	EI	EIW0105.exe	EI0105A.dll
CFST	CT	CTW0101.exe	CT0101A.dll
FAADS	FA	FAW0102.exe	FA0101A.dll
PODS	PD	PDW0105.exe	PD0105A.dll
PRMS	ME	MEW0101.exe	ME0101A.dll
SPPS	SX	SXW0101.exe	SX0101A.dll
WTWO	UU	U UW0101.exe	UU0101A.dll



## Summary

So far, we've discussed the system requirements for operating NFC's Upgrade applications. This included hardware, software, telecommunications, security, download procedures, installation procedures, and activation of the [NFC Logon client](#).

In the next section, we'll discuss how to [troubleshoot](#) common errors encountered when logging into NFC and activating individual applications. We'll also provide more information about setting up and using specific applications.

---

Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Troubleshooting Error Messages

[Common Error Messages](#)  
[Defects and Enhancements](#)  
[Summary](#)

---



## Common Error Messages

As with any software, NFC's Upgrade applications provide error messages to notify you of system problems, provide you with additional information on a process, or indicate when action is required to resolve an issue. These errors can be broken into two main categories.

### Logon and Data Access Errors

The following are messages you might encounter when using the NFC Logon Client, or starting an Upgrade Application:

- Q: When I try to logon to NFC, I get the message "TIRM629E: Error Client Manager could not send data to server."
- A: If NFC's Customer Support (CS) or other NFC personnel can log into the application and the customer has a firewall, the problem is with the customer's firewall (they should contact their agency IT personnel). If CS cannot log into the application, contact NCC to check system availability.
- Q: While in an application, I get the message "TIRM630E: Error Client Manager could not send data to server."
- A: The customer has closed the Logon window, and terminated the connection to the NFC server. They will need to close any open NFC applications and logon again.
- Q: When I try to login to an NFC application or access information, I get the message "TIRM727E: Error security not valid" or "ID has been revoked"
- A: (1) Check to ensure that your mainframe ID, password and server were entered correctly. If your password is correct,  
 (2) Contact your Agency Security Officer. The ID may be suspended, or you may not have the right security access for the action you are trying to complete.
- Q: While in an application, I get an error window containing some or all of the following text:  
 "DSNT#### SQLCODE = - 805, ERROR: DBRM OR PACKAGE NAME...."
- A: An "805" message indicates a bind error. Customer Support personnel should call the Payroll/Personnel Upgrade team with a copy of the entire error message.

### Application Errors

The following messages may occur in all Upgrade system applications. Here, NAME represents the specific application running when the error occurs (e.g., EARN, EPIC, PODS):

**AAA999999: (NAME) Application Error -- Wrong Version Installed -- Contact Info Center**

Client login attempts to verify that your version of software is correct one; if it is not, you will get this error, and should contact your Information Technology personnel. Obtain a new version of the software.

AAA9999999: (NAME) Application Error -- Navigation Table Error -- Contact Info Center

NFC Database problem; Customer Support personnel should call the Payroll/Personnel Upgrade team.

When trying to add/update a specific record, the following messages appear:

Violation of Installation Defined Edit or Validation Procedure DB60VAL

DSNT####SQLCODE = -652, ERROR: DBRM or PACKAGE NAME...

NFC Database problem; Customer Support personnel should call the Payroll/Personnel Upgrade team.

---



## Defects/Enhancements

The following items were addressed in the development and testing of these systems. These issues will/will not be implemented for the reasons provided:

- All Windows: Unable to maximize or expand the top window after using Tile or Cascade: Design of the application system permits the client to maximize only the main menu window. We do not anticipate changing this design as it would cause a complete redesign of all windows.
  - All Windows: Unable to click "X" to close or exit: Design of the application system permits the client to exit all non-banner windows using the Close button only. We do not anticipate changing this design as it would cause a complete redesign of all windows.
- 



## Summary

This section discussed errors common to the Logon client, telecommunications, and all Upgrade applications. In the next section, we'll discuss errors encountered when using specific [applications](#), as well as special things to consider when using certain applications.

---



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Application-Specific Information

This section contains information that pertains to individual applications. For issues common to all applications, reference the earlier sections of this document.

NOTE: This chapter is intended to supplement information found in the online help, directives, online tutorials, and application-specific reference guides. For detailed information on using each application, please consult these resources. For more information on where to find application documentation and help, contact [NFC Customer Support](#) at (504) 255-5230.

[\(EARN\) Earnings and Leave Statement System](#)

[\(EPIC\) Entry Processing Inquiry and Correction System](#)

[\(FAADS\) Federal Assistance Awards Database System](#)

[\(PODS\) Personnel Office Desktop Solutions](#)

[\(WTWO\) W-2 System](#)

[Summary](#)

---



## Earnings and Leave Statement System (EARN)

### Application Components

- EARN: Main Application

### General Work Flow

- Agency Security Officer sends NFC Security request for access to EARN for each user.
- Agency installs NFC Logon client on each user's PC.
- Agency installs EARN application on each PC or on a common LAN drive.
- Once NFC Security is established, users logon and start the EARN application.

### Special Considerations

There are no special considerations for using this application.

### Application-Specific Questions

Q: When I try to logon to EARN, I get the message "TIRM629E: Error client manager could not send data to server." What do I do?

A: If the EPIC banner window appears but the Menu Item options are grayed out, this could mean (1) there is a problem with your TCP/IP connection to NFC's servers, or (2) NFC's servers are unavailable. Contact your IT office.

### Technical Specifications

Files installed by the EARN Client:

- enw0101.dll
- enw0101.exe
- enw0101.ini
- wre410n.dll
- enw0101.hlp
- enw0101.reg
- enw0101h.reg

- enw0101.doc
  - EarnRead.txt
- 

## Entry Processing Inquiry and Correction System (EPIC)

### Application Components

- EPIC: Main Application

### General Work Flow

- Agency Security Officer sends NFC Security request for access to EPIC for each user.
- Agency installs NFC Logon client on each user's PC.
- Agency installs EPIC application on each PC or on a common LAN drive.
- Once NFC Security is established, users logon and start the EPIC application.

### Special Considerations

- There are no special considerations for using this application.

### Application-Specific Questions

Q: When I try to logon to EPIC, I get the message "TIRM629E: Error client manager could not send data to server." What do I do?

A: If the EPIC banner window appears but the Menu Item options are grayed out, this could mean (1) there is a problem with your TCP/IP connection to NFC's servers, or (2) NFC's servers are unavailable. Contact your IT office.

### Technical Specifications

Files installed by the EPIC Client:

- ei0105a.dll
  - eiw0105.exe
  - eiw0105.exe
  - eiw0105.ini
  - wre410n.dll
  - epic.cnt
  - epic.gid
  - epic.hlp
  - eiw0105.reg
  - eiw0105h.reg
  - eiw0105.doc
  - EpicRead.txt
-





## Federal Assistance Award Data System (FAADS)

### Application Components

- FAADS: Main Application

### General Work Flow

- Agency Security Officer sends NFC Security request for access to FAADS for each user.
- Agency installs NFC Logon client on each user's PC.
- Agency installs FAADS application on each PC or on a common LAN drive.
- Once NFC Security is established, users logon and start the FAADS application.

### Special Considerations

- There are no special considerations for using this application.

### Application-Specific Questions

Q: When I try to logon to FAADS, I get the message "TIRM629E: Error client manager could not send data to server." What do I do?

A: If the FAADS banner window appears but the Menu Item options are grayed out, this could mean (1) there is a problem with your TCP/IP connection to NFC's servers, or (2) NFC's servers are unavailable. Contact your IT office.

### Technical Specifications

Files installed by the FAADS Client:

- faw0103.dll
- faw0103.exe
- faw0103.ini
- wre410n.dll
- faad.cnt
- faad.gid
- faad.hlp
- faw0103.reg
- faw0103h.reg
- faw0103.doc
- FaadRead.txt



## Personnel Office Desktop Solutions (PODS)

### Application Components

- PODS: Main Application
- PODS – Auto Notification: Notify utility for PODS requests assigned to the user currently logged in at the workstation.
- PRMS: The Permissions System; used by the System Administrator/Security Officer at the agency to establish an employee as a user of PODS and to assign PODS profiles. The profiles determine which features of PODS the user may access, and controls view capabilities for certain types of information. To be a registered user of

PODS, the employee must exist in EMCP.

- EMCP: The Employee System; used by the PODS application to retrieve employee information from the system for a personnel request. Also used by authorized PODS users to add and maintain employee information.

## General Work Flow

- Agency Security Officer sends NFC Security request for access to PRMS for the Systems Administrator.
- Agency IT personnel install PRMS on the Systems Administrator's PC in preparation of establishing valid user IDs and profiles.
- Agency Security Officer sends NFC Security request for access to PODS and EMCP for each user.
- Agency installs NFC Logon client on each user's PC.
- Agency installs PODS application on each PC or on a common LAN drive.
- Systems Administrator establishes valid user IDs and profiles in PRMS. Available profiles are Requestor, Approver, Classifier, Staffing, and Read-Only.
- Once NFC Security and PRMS profiles are established, users logon and start the PODS application.

## Special Considerations

Because PODS uses two types of security (NFC system security and agency-specified profile access), it is helpful to know which type of message is being sent when an error is encountered:

- If the error window title bar displays a "PD" number (e.g., PD0103), this error is from the PODS Client. Reference the PODS Online Help for more information about resolving the error. If the error provides a resolution such as the one listed below, consult the agency System Administrator or Security Officer for help.
- If the error window title bar displays simply "Error" and a series of numbered lines, users should refer to the [Troubleshooting](#) section of this document to determine the meaning of the error and the appropriate point-of-contact.

## Application-Specific Questions

Q: I logged into NFC, started PODS and saw "YOU ARE NOT REGISTERED AS A USER OF PODS. YOU NEED TO GET YOURSELF SETUP AND AUTHORIZED TO USE PODS." What do I do?

A: Contact your agency Systems Administrator or Point-of-Contact for PODS. You need to be established in the PRMS system as an authorized user of PODS.

## Technical Specifications

Files installed by the PODS Clients:

PODS Client	<ul style="list-style-type: none"> <li>• mow00.dll</li> <li>• pdw0105.dll</li> <li>• pdw0105.exe</li> <li>• pd0105z.exe</li> <li>• wre410n.dll</li> <li>• pd0105z.bck</li> <li>• mow01.dll</li> <li>• mow01.exe</li> <li>• mow01.reg</li> <li>• mow02.dll</li> <li>• mow02.exe</li> <li>• mow02.reg</li> <li>• pd0105z.ini</li> <li>• pdw0105.ini</li> </ul>	<ul style="list-style-type: none"> <li>• ticontrols.ocx</li> <li>• dao.reg</li> <li>• pd0105a.dll</li> <li>• pd0105b.dll</li> <li>• pd0105c.dll</li> <li>• pd0105d.dll</li> <li>• pd0105e.dll</li> <li>• pd0105f.dll</li> <li>• pd0105g.dll</li> <li>• pd0105h.dll</li> <li>• pd0105i.dll</li> <li>• pd0105j.dll</li> <li>• pd0105k.dll</li> <li>• pd0105l.dll</li> </ul>	<ul style="list-style-type: none"> <li>• pd0105n.dll</li> <li>• pd0105o.dll</li> <li>• pd0105z.dll</li> <li>• pods.cnt</li> <li>• pods.gid</li> <li>• pods.hlp</li> <li>• pd0105z.reg</li> <li>• pdw0105.reg</li> <li>• pdw0105h.reg</li> <li>• pdw0105.bat</li> <li>• pdw0105.doc</li> <li>• PodsRead.txt</li> </ul>
-------------	--	---	---

		<ul style="list-style-type: none"> <li>● pd0105m.dll</li> </ul>	
EMCP Client	<ul style="list-style-type: none"> <li>● ec0105a.dll</li> <li>● ecw0105.exe</li> <li>● ecw0105.exe</li> <li>● ecw0105.ini</li> </ul>	<ul style="list-style-type: none"> <li>● wre410n.dll</li> <li>● emcp.cnt</li> <li>● emcp.gid</li> <li>● emcp.hlp</li> </ul>	<ul style="list-style-type: none"> <li>● ecw0105.reg</li> <li>● ecw0105h.reg</li> <li>● ecw0105.doc</li> <li>● EmcpRead.txt</li> </ul>
PRMS Client	<ul style="list-style-type: none"> <li>● mew0101.dll</li> <li>● mew0101.exe</li> <li>● mew0101.ini</li> </ul>	<ul style="list-style-type: none"> <li>● wre410n.dll</li> <li>● prms.cnt</li> <li>● prms.gid</li> <li>● prms.hlp</li> </ul>	<ul style="list-style-type: none"> <li>● mew0101.reg</li> <li>● mew0101h.reg</li> <li>● mew0101.doc</li> <li>● PrmsRead.txt</li> </ul>
PODS Reports	<ul style="list-style-type: none"> <li>● pdc10rpt.exe</li> <li>● pdc10rpt.crf</li> <li>● pdc10rpt.mdb</li> <li>● pdc10rpt.rpt</li> <li>● pdc1rpt.exe</li> <li>● pdc1rpt.crf</li> <li>● pdc1rpt.mdb</li> <li>● pdc1rpt.rpt</li> <li>● pdc2rpt.exe</li> <li>● pdc2rpt.crf</li> <li>● pdc2rpt.mdb</li> <li>● pdc2rpt.rpt</li> <li>● pdc4rpt.exe</li> <li>● pdc4rpt.crf</li> <li>● pdc4rpt.mdb</li> <li>● pdc4rpt.rpt</li> <li>● pdc7rpt.exe</li> <li>● pdc7rpt.crf</li> <li>● pdc7rpt.mdb</li> <li>● pdc7rpt.rpt</li> <li>● pdcVacAn.exe</li> <li>● pdcVacAn.crf</li> <li>● pdcVacAn.mdb</li> <li>● pdcVacAn.rpt</li> </ul>	<ul style="list-style-type: none"> <li>● pdEval.exe</li> <li>● pdEval.crf</li> <li>● pdEval.mdb</li> <li>● pdEval.rpt</li> <li>● pdEval2.exe</li> <li>● pdEval2.crf</li> <li>● pdEval2.mdb</li> <li>● pdEval2.rpt</li> <li>● pdInelig.exe</li> <li>● pdInelig.crf</li> <li>● pdInelig.mdb</li> <li>● pdInelig.rpt</li> <li>● pdnotify.exe</li> <li>● pdnotsel.crf</li> <li>● pdnotsel.mdb</li> <li>● pdnotsel.rpt</li> <li>● pdreceipt.exe</li> <li>● pdreceipt.crf</li> <li>● pdreceipt.mdb</li> <li>● pdreceipt.rpt</li> <li>● pdreceipt2.rpt</li> </ul>	<ul style="list-style-type: none"> <li>● crpe32.dll</li> <li>● msvcrt20.dll</li> <li>● crpaig32.dll</li> <li>● ctL3D32.dll</li> <li>● implode.dll</li> <li>● crrun32.dll</li> <li>● p2bdao.dll</li> <li>● p2ctdao.dll</li> <li>● p2irdao.dll</li> <li>● dao2535.tlb *</li> <li>● vbajet32.dll</li> <li>● ven2232.olb *</li> <li>● msjt3032.dll</li> <li>● vbar332.dll</li> <li>● msrd2x35.dll</li> <li>● msjint35.dll</li> <li>● msjter35.dll</li> <li>● dao350.dll *</li> <li>● mfc30.dll</li> <li>● mfc42.dll *</li> <li>● msvcrt.dll</li> <li>● msvcrt40.dll</li> <li>● oleaut32.dll *</li> <li>● msjet35.dll *</li> </ul>
* Self-registering Files			



## W-2 System (WTWO)

### Application Components

- WTWO: Main Application
- WTWO Reports: Reports generating utility

### General Work Flow

- Agency Security Officer sends NFC Security request for access to WTWO for each user.

- Agency installs NFC Logon client on each user's PC.
- Agency installs WTWO application on each PC or on a common LAN drive.
- Agency installs WTWO Reports on each user's PC.
- Once NFC Security is established, users logon and start the WTWO application.

## Special Considerations

There are no special considerations for this application.

## Application-Specific Questions

**Q:** When I try to logon to WTWO, I get the message "TIRM629E: Error client manager could not send data to server." What do I do?

**A:** If the WTWO banner window appears but the Menu Item options are grayed out, this could mean (1) there is a problem with your TCP/IP connection to NFC's servers, or (2) NFC's servers are unavailable. Contact your IT office.

## Technical Specifications

Files installed by the WTWO Clients:

WTWO Client	<ul style="list-style-type: none"> <li>● uuw01.dll</li> <li>● uuw01.exe</li> <li>● uuw01.ini</li> <li>● wre410n.dll</li> </ul>	<ul style="list-style-type: none"> <li>● wtwo.cnt</li> <li>● wtwo.gid</li> <li>● wtwo.hlp</li> <li>● uuw01.reg</li> </ul>	<ul style="list-style-type: none"> <li>● uuw01h.reg</li> <li>● uuw01.doc</li> <li>● WtwoRead.txt</li> </ul>
WTWO Reports Client	<ul style="list-style-type: none"> <li>● uu30.exe</li> <li>● uu30.crf</li> <li>● uu30.mdb</li> <li>● uu30.rpt</li> <li>● uu90rpt.exe</li> <li>● uu90rpt.crf</li> <li>● uu90rpt.mdb</li> <li>● uu90rpt.rpt</li> <li>● dao.reg</li> <li>● crpe32.dll</li> <li>● msvcr20.dll</li> <li>● crpaig32.dll</li> </ul>	<ul style="list-style-type: none"> <li>● ctL3D32.dll</li> <li>● implode.dll</li> <li>● crrun32.dll</li> <li>● p2bdao.dll</li> <li>● p2ctdao.dll</li> <li>● p2irdao.dll</li> <li>● dao2535.tlb *</li> <li>● vbajet32.dll</li> <li>● ven2232.olb *</li> <li>● msjt3032.dll</li> <li>● vbar332.dll</li> <li>● msrd2x35.dll</li> </ul>	<ul style="list-style-type: none"> <li>● msjint35.dll</li> <li>● msjter35.dll</li> <li>● dao350.dll *</li> <li>● mfc30.dll</li> <li>● mfc42.dll *</li> <li>● msvcr20.dll</li> <li>● msvcr40.dll</li> <li>● oleaut32.dll *</li> <li>● msjet35.dll *</li> </ul>
* Self-registering Files			



## Summary

More information on these applications may be found in the online help, tutorials and "readme" documentation provided for each.

The remaining sections will contain [technical information](#) targeted to help IT/IS personnel within your agency to setup, maintain, and troubleshoot these systems.



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Technical Information

This section is provided for technical support and IT personnel at your agency. It is intended to furnish information of a specific and technical nature that may assist these personnel with setting up, maintaining and troubleshooting the client portion of NFC's Upgrade Systems. For more information on setting up and using these systems, please see earlier chapters of this guide.

[Minimum System Requirements](#)

[Local System Changes](#)

[Communications Software](#)

[Summary](#)



## Minimum System Requirements

Depending upon your PC system's configuration, the system requirements for running NFC Upgrade applications may vary. As a minimum benchmark, we recommend the following:

RAM:	Same as required to run your operating system.
NFC Logon Client:	Approximately 5MB of available disk space on the C: drive.
Application Clients:	The disk space requirements for individual applications will vary. Consult the application's Readme file for specifics.

For more information on general system setup recommendations, see [Getting Started](#).



## Local System Changes

When the NFC Logon client is installed, several changes are made to the local PC system. Folders are added, and registry entries are added or modified. Depending on where the application clients are installed, certain changes may be made to LAN drives as well. This section will detail any changes made during installation of NFC clients.

### Folders Created by Installed Clients

Installation of the NFC Logon client will create the following folders on the C:\ drive:

USDANFC\	Root folder for all NFC applications
USDANFC\ Bin	Empty on install; used by the Logon client; see Files Installed by the Application Clients
USDANFC\ NFCLogon	Contains program files for the Logon client
USDANFC\ NFCApps	Empty on install; used for local installation of NFC Application clients, and for data storage by certain application clients.
USDANFC\ Reports	Empty on install; used by application clients to store system report generators.

Installation of the Application clients will copy all application executables and program files into the existing NFCApps folder. If the applications are installed to a LAN drive, the installation program will create an NFCApps folder in the destination directory specified during installation.

## Files Installed by the NFC Logon Client

The NFC Logon Client installation copies several Dynamic Link Library (DLL) files into two folders. Most of these DLLs (also called runtime libraries) are deployed into the C:\USDANFC\NFCLogon folder. However, some MS Visual C++ runtimes are deployed into the Windows\System directory. They are:

- Mfc42.dll
- Msvcr7.dll
- Mfc40.dll
- Msvcr70.dll
- Msvcr70.dll
- Msvcr7.dll
- Olepro32.dll
- Oleaut32.dll
- Ssfm1032.dll

The automated setup handles the installation of these files. The setup will copy the files if they don't exist on the installation system, or overlay existing files if they are older than the ones being installed. There are no system runtimes installed with the individual applications. Application installs include only the application files, which are loaded into the destination directory selected during setup. When the applications are started from the [Logon Client](#), they will use all runtimes installed by the Logon System.

### The Registry

In addition to copying files into the Windows\System or NFCLogon folders, the InstallShield installation program also registers several files. They are:

- Wru410n.dll
- Wroa0000.tlb
- Wrof0000.tlb
- Mfc42.dll
- Mfc40.dll
- Olepro32.dll
- SSFM1032.dll

- Lgw0101.reg

## Files Installed by the Application Clients

As mentioned, no runtimes are added to the System folder during Application client installations. However, when an application is started for the first time, several files will be copied to the Bin folder created by the NFC Logon client install. In this operation, the Logon client searches the application path specified by the user, locates these files, edits them, copies the updated files to the Bin folder, and, in the case of \*.reg and \*.bat files, executes them.

### \*.reg files

Every application client has two registry files, one for the main application executable and one for the help files. Their primary purpose is to register the associated application's installed location. The reg files have only the default directory as the path to be registered. If you installed the applications to a LAN folder, these paths would need to be modified for the Logon start to work properly. NFC does this for you with the Start function.

When the Logon client locates an application's reg file, it looks for any instance of the application path,

and edits it to match the application path currently specified in the Logon client window (see Chapter 5, The NFC Logon Client: Changing the Application Path). It then runs the reg file and updates the PC's registry with the current path to the installed application.

This will also take place any time the path is changed in the Logon client. When an application is started after a path change, it will re-register itself automatically. This ensures that applications will always be updated and properly referenced.

#### \*.ini files

Every application also has an ".ini" file, which contains the path to which the Logon client was pointing when the application was started. Subsequently, this file will be updated every time the Logon client application path is changed.

#### \*.bat files

Some applications have an extra file, which is used to perform registrations unique to that application. One example is PODS, which uses a ".bat" file to register a proprietary OCX file.

#### Application Start Filenames

As mentioned, all of the above files may be found in the C:\USDANFC\BIN folder. To determine which files belong to which application, follow the naming convention provided in [System Maintenance](#).

AAW0101.reg	Primary executable's path
AAW0101h.reg	Help file's path
AAW0101.ini	Application's *.ini file
AAW0101.bat	Application's *.bat file

You may view the contents of these files at any time to determine where the applications were last registered.



## Communications Software

The NFC Logon client utilizes a behind-the-scenes telecommunications application called Client Manager. This application is activated when the user enters their ID and Password and clicks Logon. All communications settings are pre-configured upon installation of the Logon client, so the system has the Host Name and Port information to properly connect to NFC servers. Client Manager runs in the background, invisible to users, but may be accessed by doing the following:

- With the Logon client running, enter your ID and password. The Logon button becomes active.
- Click Logon.
- Make sure the Logon window is active, then press CTRL+SHIFT+S.

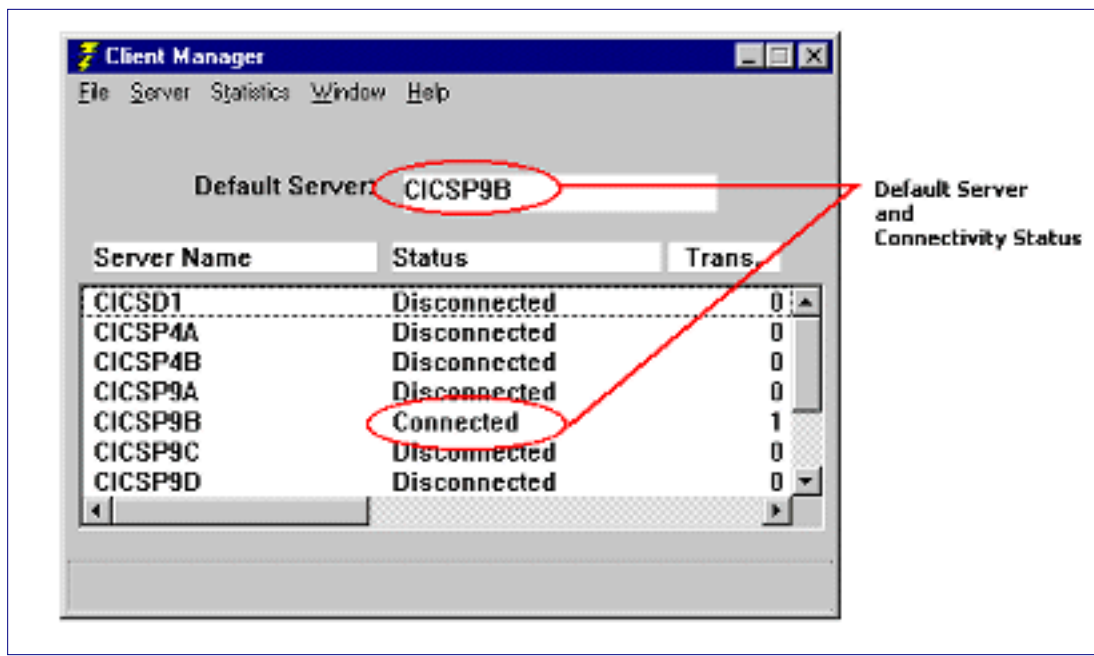
The Client Manager window appears in the taskbar. Click to restore it to full size. If at any time you need to hide the Client Manager window, make sure the Logon window is active, then press CTRL+SHIFT+H.

### Using Client Manager

Because Client Manager is pre-configured to connect to NFC, you will most likely only use this section when trying to determine if you have the latest version of the NFC Logon system installed, or when troubleshooting connectivity to NFC.

#### The Client Manager Window





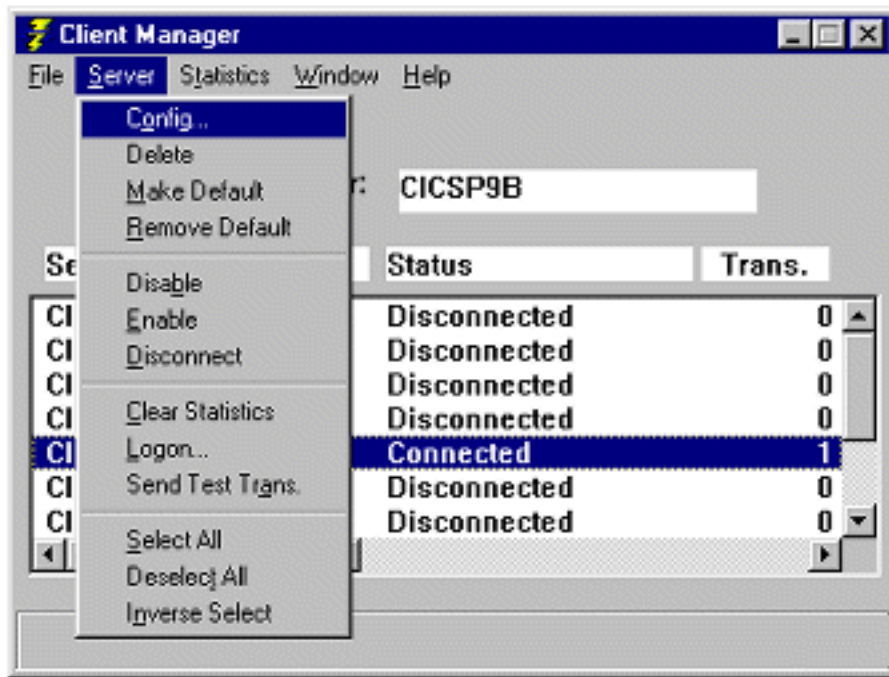
From this window, you may view the connectivity settings for all NFC servers. This includes server configuration, logon status, and transaction statistics.

Note the Default Server. For systems with multiple servers, like Payroll/Personnel, one IP Address will have several valid ports, one for each server name. When a user selects a server on the Logon window, Client Manager connects to the first available server and port matching the configuration requirements. In the above illustration, the user selected Payroll/Personnel as the Server, and Client Manager negotiated a connection to the CICSP9B server. If the user had selected QA Testing as the Logon server, the Default Server would Display CICSQA.

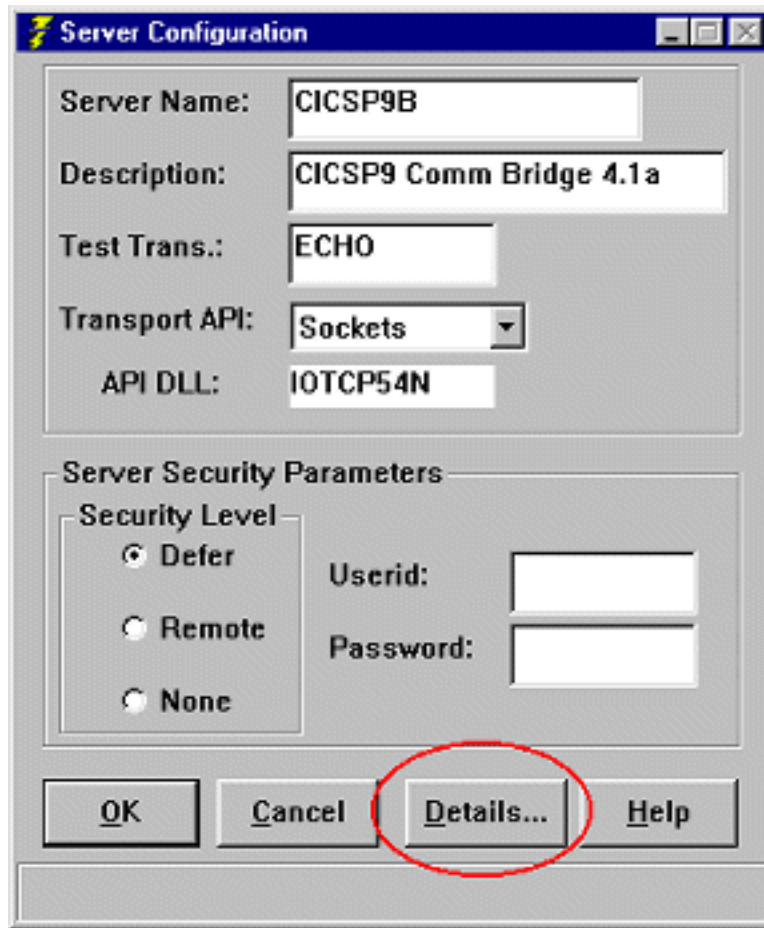
The Logon client's server options and their corresponding server names are listed below:

Logon Server Selection	Client Manager Server Name
Training	CICSD1
Administrative	CICSP4A and B
Payroll/Personnel	CICSP9A through E
Parallel 1	Not Assigned
Parallel 2	Not Assigned
QA Testing	CICSQA
Test 4 (NFC Only)	CICST4
Test 9 (NFC Only)	CICST9

To see the actual host and port settings, use the menu option Server > Config....

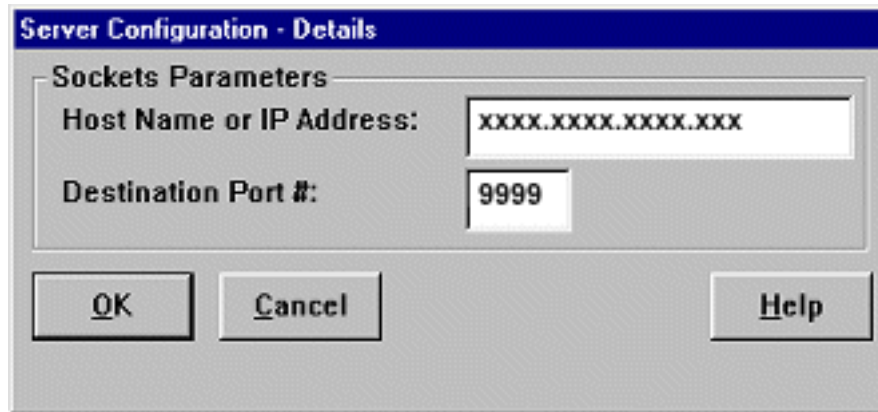


The Server Configuration window contains the general settings for the selected server. To view the specific IP Address and port connections, click the Details button.



In the Details window, you can see the current settings being used by the Logon client to connect to NFC.

If you are having connectivity problems, this is where you would get the information NFC needs to determine if your system's server settings are up-to-date.



**Server Configuration - Details**

**Sockets Parameters**

Host Name or IP Address:

Destination Port #:

You can find more detailed information on other features and functions of Client Manager by accessing the online help for that application.

---

## Summary

If you wish to review any of the information discussed thus far, select from the navigation bar, or browse the [Appendix](#) and [Glossary](#).



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# Appendices

- A. [Connecting to NFC via TCP/IP](#): Listing of options and descriptions for the five methods of establishing secured TCP/IP Connection with NFC.
  - B. [Links and Other Resources](#)
- 



## APPENDIX A – Connecting to NFC via TCP/IP

[Option A: Establishing a Firewall to Firewall Connection](#)

[Option B: Establishing a Gateway to Gateway Connection](#)

[Option C: Establishing a SecuRemote Client to Checkpoint Firewall Connection](#)

[Option D: Establishing an Entrust/SecuRemote Client to NFC Connection](#)

[Option E: Establishing a Direct Connection \(Line/Router\)](#)

---



### Option A: Establishing a Firewall to Firewall Connection

- Create a virtual private network (VPN) between customer's firewall and NFC's IBM Firewall (Version 4.2)
    - a. Obtain customer firewall type and version.
    - b. Exchange IP addresses (Customer and NFC/ISSO)
      - i. Establish valid host and port connection
      - ii. Distinguish between Firewall IP addresses and Network addresses
    - c. Configure customer's Firewall and routing tables.
    - d. Update NFC's Firewall and routing tables.
  - Coordinate TCP/IP Application Testing (ISSO)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate customer's ability to reach the NFC sign-on screen (TN3270) or EARN main screen (CoolGen app), and ability to complete a File Transfer to NFC's Mainframe.
  - Coordinate NFC Application Testing (IC)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate operation of specific applications (EARN, IRIS, Travel) and telecommunication clients (TN3270, FTP, VPS Print, CoolGen) via Firewall to Firewall connection.
  - Implement Into Production
-



## Option B: Establishing a Gateway to Gateway Connection

- Create a VPN between customer's network and NFC's network terminating at NFC's TimeStep/PERMIT Gateway (Version 1.10)
    - a. Procure/install TimeStep/PERMIT Gateway on Customer's network
    - b. Exchange IP addresses (Customer and NFC/ISSO)
      - i. Establish valid host and port connection
      - ii. Distinguish between Firewall IP addresses and Network addresses
    - c. Configure customer's PERMIT Gateway, firewall, and routing tables.
    - d. Update NFC's PERMIT Gateway, firewall, and routing tables.
  - Coordinate TCP/IP Application Testing (ISSO)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate customer's ability to reach the NFC sign-on screen (TN3270) or EARN main screen (CoolGen app), and ability to complete a File Transfer to NFC's Mainframe.
  - Coordinate NFC Application Testing (IC)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate operation of specific applications (EARN, IRIS, Travel) and telecommunication clients (TN3270, FTP, VPS Print, CoolGen) via Gateway to Gateway connection.
  - Implement Into Production
- 



## Option C: Establishing a SecuRemote Client to Checkpoint Firewall Connection

- Create a VPN between customer's desktop and NFC's network terminating at Checkpoint Firewall
  - a. Request client on Customer's Windows 95 and/or NT desktops
    - i. Windows 95B (Version 4.00.950B), 32 Meg RAM
    - ii. Windows NT with Service Pack 3, 64 Meg RAM
    - iii. NOTE: Customers whose network is located behind a firewall running NAT will require a static route in their firewall to allow their network to communicate with NFC. This will take coordination of both the Customers and NFC Firewall Managers. Prior to proceeding initiate this communication.
  - b. Set up SecuRemote Client
    - i. Receive and follow the download of software instructions
    - ii. Establish the SecuRemote Client
- Coordinate TCP/IP Application Testing (ISSO)
  - a. a. Establish test criteria

- b. b. Set testing dates
    - c. c. Test and evaluate customer's ability to reach the NFC sign-on screen (TN3270) or EARN main screen (CoolGen app), and ability to complete a File Transfer to NFC's Mainframe.
  - Coordinate NFC Application Testing (IC)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate operation of specific applications (EARN, IRIS, Travel) and telecommunication clients (TN3270, FTP, VPS Print, CoolGen) via Client to Gateway connection.
  - Implement Into Production
- 



#### Option D: Establishing an Entrust/SecuRemote Client to NFC Connection

- Create a VPN between customer's desktop and NFC
  - a. Procure/request client on Customer's Windows 95 and/or NT desktops
    - i. Windows 95B (Version 4.00.950B), 32 Meg RAM
    - ii. Windows NT with Service Pack 3, 64 Meg RAM
    - iii. NOTE: Customers whose network is located behind a firewall running NAT will require a static route in their firewall to allow their network to communicate with NFC. This will take coordination of both the Customers and NFC Firewall Managers. Prior to proceeding initiate this communication.
    - iv. Customer must present pictured identification along with a signed subscriber agreement.
    - v. The client request, pictured ID, and subscriber agreement along with the users NFC ID, e-mail address and phone number are forwarded to NFC by the NFC Security Officer.
  - b. Set up the Entrust/SecuRemote Client
    - i. Receive and follow the download of software instructions
    - ii. Establish the Entrust/SecuRemote Client
    - iii. Activate the Client Digital Signature Certificate
- Coordinate TCP/IP Application Testing (ISSO)
  - a. Establish test criteria
  - b. Set testing dates
  - c. Test and evaluate customer's ability to reach the NFC sign-on screen (TN3270) or EARN main screen (CoolGen app), and ability to complete a File Transfer to NFC's Mainframe.
- Coordinate NFC Application Testing (IC)
  - a. Establish test criteria
  - b. Set testing dates
  - c. Test and evaluate operation of specific applications (EARN, IRIS, Travel) and telecommunication clients (TN3270, FTP, VPS Print, CoolGen) via Client to Gateway

connection.

- Implement Into Production



#### Option E: Establishing a Direct Connection (Line/Router)

- Establish a true private network connection between customer's network and NFC's network terminating at NFC's CISCO Router (border router)
    - a. Provide serial port on customer's CISCO router and serial link between customer network and NFC. NOTE: Customers must have a CISCO router to use this option.
    - b. Configure customer's router, firewall, and routing tables.
    - c. Update border router, firewall, and routing tables.
  - Coordinate TCP/IP Application Testing (ISSO)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate customer's ability to reach the NFC sign-on screen (TN3270) or EARN main screen (CoolGen app), and ability to complete a File Transfer to NFC's Mainframe.
    - d.
  - Coordinate NFC Application Testing (IC)
    - a. Establish test criteria
    - b. Set testing dates
    - c. Test and evaluate operation of specific applications (EARN, IRIS, Travel) and telecommunication clients (TN3270, FTP, VPS Print, CoolGen) via Direct connection.
  - Implement Into Production
- 



## APPENDIX B – Other Resources and Links

Several resources are available to NFC customers. The first point of contact should always be your NFC Customer Service Representative. They may then point you to one of the following resources:

- There is invaluable information to be found on the NFC Home Page. [Contact lists](#), [Frequently Asked Questions](#), and more may be found by pointing your browser to [www.nfc.usda.gov](http://www.nfc.usda.gov)
- For information on using NFC applications, contact Customer Support at (504) 255-5230.
- For information on printed directives, application help, and other publications, contact the Directives and Analysis Branch.
- Send us Email:
  - Customer Support Office: [customer.support@usda.gov](mailto:customer.support@usda.gov)

- Directives and Analysis Branch: [nfc.dab@usda.gov](mailto:nfc.dab@usda.gov)
- Feedback for this website: [nfc.webmaster@usda.gov](mailto:nfc.webmaster@usda.gov)



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) 11 [12](#) [13](#)



# Glossary

---

## application client:

Software loaded on a local or network drive that provides the application environment (windows) for accessing and processing data. Examples: EARN, EPIC, PODS.

## batch processing:

A type of computer processing in which a batch of requests is stored and then executed all at one time. Transaction processing requires interaction with a user, whereas batch processing can take place without a user being present.

## bind:

To assign a value to a symbolic placeholder. During compilation, for example, the computer assigns symbolic addresses to some variables and instructions. When the program is bound, or linked, the binder replaces the symbolic addresses with real machine addresses. The moment at which binding occurs is called bind time or link time.

## CICS:

(Customer Information Control System) A TP monitor from IBM that was originally developed to provide transaction processing for IBM mainframes. It controls the interaction between applications and users and lets programmers develop screen displays without detailed knowledge of the terminals being used.

## database server:

Software maintained by NFC to house customer information. Accessed remotely from the customer site using client software.

## firewall:

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Types of firewall techniques include: Packet filter; application gateway; circuit-level gateway; proxy server.

## logon client:

Software that links the application client to the NFC system. Used to logon to NFC's database servers, verify user security access, and display all available applications. Starting point of the telecommunications connection to NFC.

## node:

In networks, a processing location. A node can be a computer or some other device, such as a printer. Every node has a unique network address (e.g., DLC or MAC addresses).

## PING:

A utility to determine whether a specific IP Address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

secured link :

Established in one of several ways, generally involving a direct connection, firewalls, or a separate encryption client, any of which protects transmitted data from being compromised by non-authorized users. Required to operate all NFC Upgraded applications.

transaction processing:

A type of computer processing in which the computer responds immediately to user requests. Each request is considered to be a transaction. Automatic teller machines for banks are an example of transaction processing. The opposite of transaction processing is batch processing.

VTAM:

(Virtual Telecommunications Access Method) The software component that controls communications in SNA networks. VTAM supports several network protocols.



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)

# FAQs

---

- [What systems will the upgrade applications replace or enhance?](#)
  - [How do I know if my agency has a secured TCP/IP connection to NFC?](#)
  - [How do I know when an update to an application client needs to be installed?](#)
  - [Do I need a new ID to access these applications?](#)
  - [Where can I find help on using each application?](#)
- 



What systems will the upgrade applications replace or enhance?

- EARN replaces the existing Earnings and Leave Statement System, which was formerly unavailable for remote inquiry.
- EPIC replaces PACT, PRES, SING, FINQ, HCUP and PEP51.
- FAAD replaces the existing blockmode Federal Awards Assistance Data system.
- PODS automates the existing paper process of personnel management, primarily the SF-72 process and recruitment. It does not replace an existing system.
- WTWO replaces the existing blockmode W2 Inquiry system.
- EMCP and PRMS are adjunct applications that provide added security and flexibility to certain upgrade applications. They are not replacing any existing systems.

When an agency or office elects to use upgrade systems, they will be switched over to access only those upgrade databases. For instance, an agency electing to use EPIC will no longer access the systems that EPIC is replacing.



How do I know if my agency has a secured TCP/IP connection to NFC?

If you don't know your agency's NFC liason, you may contact your Customer Service Representative. For a list of representatives and their agencies, goto the [NFC Home Page](#) or call (504) 255-5230.



How do I know when an update to an application client is available?

When you use the NFC Logon window and attempt to start an application that must be updated, you'll receive a notification message indicating that you should download the new setup file by a certain date. For more information, see [The NFC Logon Client](#)



Do I need a new ID to access these applications?

No. If you already have an NFC ID for other systems, your Security Officer should send in a request for security access to the desired applications. Your ID will be updated to include access to the upgrade systems you requested.



Where can I find help on using each application?

Help is available in the form of

- online help, accessed from the menu bar of each application
- printed directives, available by request from the NFC
- this guide
- technical support analysts with NFC's Customer Support (504) 255-5230.



Goto Section: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) 13

**REQUEST FOR ELECTRONIC DOWNLOADING OF SOFTWARE FROM NFC****A. IDENTIFICATION**

NAME	TELEPHONE NUMBER (Area Code and Number)
AGENCY	

**B. TYPE OF SOFTWARE REQUESTED (Check type(s) of software requested.)**

✓	SOFTWARE	SOFTWARE DEFINITION
	<b>Purchase Card Management System (PCMS)</b> (with Runtime Modules)	Includes runtime modules for Oracle forms, graphics, reports, and PCMS application forms, menus, libraries, and reports. It also includes SQL*NET and ANO configured for access to NFC. An Oracle password change form (PASSORCL) is also included, which allows users to change their password.
	<b>PCMS</b> (without Runtime Modules)	Includes PCMS application forms, menus, libraries, and reports. PASSORCL is also included, which allows users to change their password. These files are for a user who currently has Oracle forms, graphics, reports, SQL*NET, and ANO on their workstations.
	<b>PCMS</b> (with Discoverer 2000)	Includes runtime modules for Oracle forms, graphics, Discoverer 2000, and PCMS application forms, menus, libraries, reports, and the Security Access Management System (SAMS). It also includes SQL*NET and ANO configured for access to NFC. PASSORCL is also included, which allows users to change their password. For use by APC's and LAPC's.
	<b>Discoverer 2000</b>	Includes Discoverer 2000 software. PASSORCL is also included, which allows users to change their password.
	<b>Security Access Management System (SAMS)</b>	Includes SAMS application only. (SAMS allows agency security officers to electronically establish security access for specified ORACLE applications.)
	<b>PASSORCL</b>	Includes the Oracle password change form which allows users to change their password.
	<b>Consolidated Financial Statements System (CFST)</b>	CFST Windows 95/NT is used to produce the Department of Agriculture's Consolidated Financial Statements. A CFST tutorial is also available.
		Windows 95/NT applications of NFC's Payroll/Personnel Upgrade. Tutorials are also available. <i>(Type in the requested application name in the Software Column to the left; e.g., EARN, EPIC, etc.)</i>

**C. USER REQUIREMENTS****FTP CLIENT AND INTERNET CONNECTION**

Locations that do not have FTP software for use to download the above application(s) can download a free copy from the Internet. Instructions for downloading FTP software are included in the instructions provided by NFC for downloading the software requested in Section B above.

Choose only **one** of the four options below and provide the requested address/fax number to indicate where NFC should send the instructions for downloading the software.

**Requestor E-Mail Address**

AREA CODE

**Requestor Fax Number (       )****Information Technology (IT) Contact E-Mail Address**

AREA CODE

**IT Contact Fax Number (       )****D. AUTHORIZATION**

IT CONTACT NAME		
AUTHORIZED SIGNATURE AND TITLE	TELEPHONE NUMBER (Area Code and Number)	DATE

MAIL, E-MAIL, OR FAX THIS FORM TO:

AD-1128 (Revised 11/98)

**Mailing address:** DAB, National Finance Center, P.O. Box 60000, New Orleans, LA 70160**E-mail:** nfc.dab@usda.gov**Fax number:** 504-255-4367